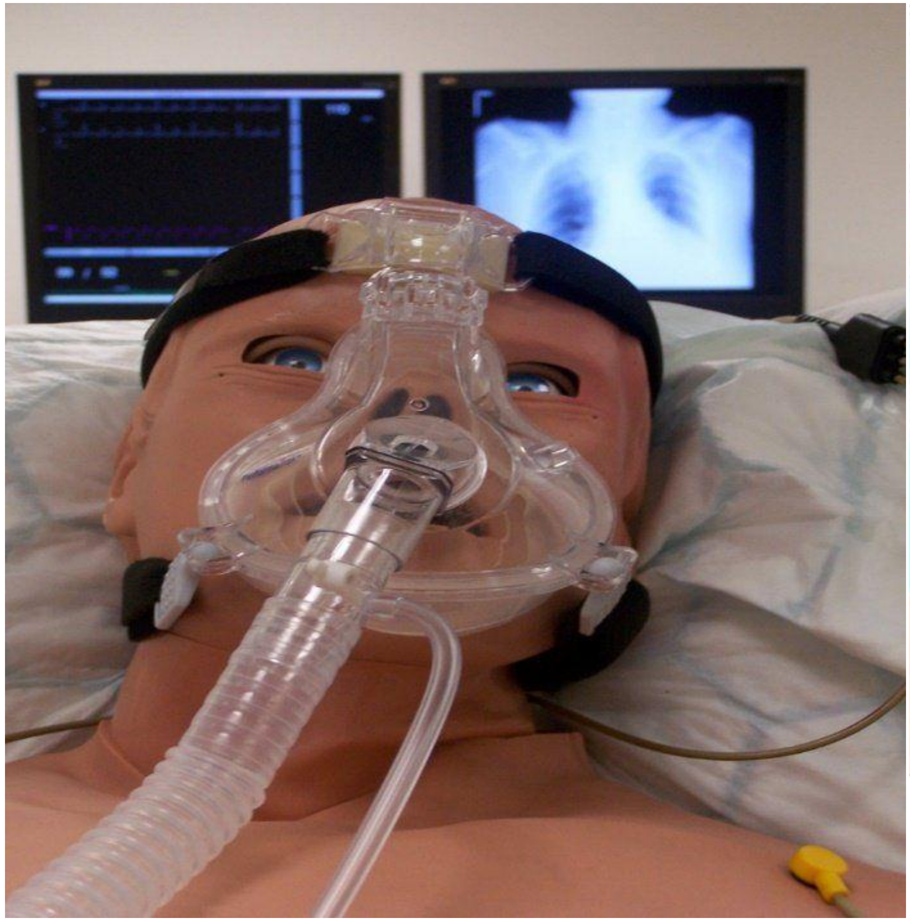
DREAD Analysis: defence and mitigation Team 3



Based on Compromising a Medical Mannequin (Glisson at al, 2015)

	Damage	Reproducibility	Exploitability	Affected Users	Discoverability	Total	Risk
Brute force: Weak password	2	3	1	2	2	10	12/5 = 2 (Moderate Risk)
Denial of Service	3	2	2	3	3	13	13/5 = 2.6 (High Risk)

Defence and mitigation

- Deactivate uPnp and WPS (BF)
- Use strong long complex alphanumeric passwords with symbols (i.e., !Afdh1.2c&) (BF)
- Never use the same or similar passwords for different accounts (BF)
- Limit the number of failed login attempts (BF)
- Use wired connection instead of wireless (BF)
- Use 2FA (BF)
- DoS attacks can be mitigated using a strong firewall (DoS)
- Use VLAN to isolate or segment network (DoS)
- Keeping firmware up to date (BF,DoS)
- Awareness training to inculcate the security culture (BF,DoS)
- Use CAPTCHA (BF)